The geometry of diagonal groups

Peter J. Cameron, University of St Andrews

ICDM, Tirunelveli
12 October 2021

Joint work with Rosemary Bailey, Michael Kinyon, Cheryl Praeger and Csaba Schneider

I am going to tell you about a theorem which I regard as one of the rare good effects of the Covid pandemic: the main theorem was proved during the first lockdown in Britain.

I am going to tell you about a theorem which I regard as one of the rare good effects of the Covid pandemic: the main theorem was proved during the first lockdown in Britain.
It started out as an attempt to describe the combinatorial structures associated with "diagonal groups", but expanded to include Latin squares, synchronizing automata, a generalisation of arcs in projective spaces, graph homomorphisms, and many other topics in discrete mathematics.

I am going to tell you about a theorem which I regard as one of the rare good effects of the Covid pandemic: the main theorem was proved during the first lockdown in Britain.
It started out as an attempt to describe the combinatorial structures associated with "diagonal groups", but expanded to include Latin squares, synchronizing automata, a generalisation of arcs in projective spaces, graph homomorphisms, and many other topics in discrete mathematics.
So welcome to the feast!

Permutation groups

Throughout, G will denote a permutation group on Ω.

Permutation groups

Throughout, G will denote a permutation group on Ω.
G is transitive if no non-trivial subset of Ω is G-invariant; it is primitive if no non-trivial partition of Ω is G-invariant. (The trivial subsets or partitions are those invariant under the symmetric group on Ω.

Permutation groups

Throughout, G will denote a permutation group on Ω.
G is transitive if no non-trivial subset of Ω is G-invariant; it is primitive if no non-trivial partition of Ω is G-invariant. (The trivial subsets or partitions are those invariant under the symmetric group on Ω.
Many (but not all) questions about permutation groups can be reduced to the case where the group is primitive. This has been a standard technique since Jordan in the 19th century.

Permutation groups

Throughout, G will denote a permutation group on Ω.
G is transitive if no non-trivial subset of Ω is G-invariant; it is primitive if no non-trivial partition of Ω is G-invariant. (The trivial subsets or partitions are those invariant under the symmetric group on Ω.
Many (but not all) questions about permutation groups can be reduced to the case where the group is primitive. This has been a standard technique since Jordan in the 19th century.
More specifically, a permutation group can be embedded in a subcartesian product of transitive groups, while a transitive group (at least in the finite case) has a similar embedding in a wreath product of primitive groups.

The O'Nan–Scott Theorem

The following theorem (and indeed rather more) was proved by Michael O'Nan and Leonard Scott (independently) in 1979. The version I need here is little more than is in Jordan's *Traité des Substitutions* – the important extra information is all in the wreath product case.

The O'Nan–Scott Theorem

The following theorem (and indeed rather more) was proved by Michael O'Nan and Leonard Scott (independently) in 1979. The version I need here is little more than is in Jordan's *Traité des Substitutions* – the important extra information is all in the wreath product case.

Theorem

A finite primitive permutation group is of one of the following types: affine, wreath product, diagonal, or almost simple.

The O'Nan–Scott Theorem

The following theorem (and indeed rather more) was proved by Michael O'Nan and Leonard Scott (independently) in 1979. The version I need here is little more than is in Jordan's *Traité des Substitutions* – the important extra information is all in the wreath product case.

Theorem

A finite primitive permutation group is of one of the following types: affine, wreath product, diagonal, or almost simple.

Affine groups preserve affine spaces; wreath products preserve Cartesian structures (as I discuss later); almost simple groups form a ragbag, and there is no hope for a uniform description of the structures they act on.

The O'Nan–Scott Theorem

The following theorem (and indeed rather more) was proved by Michael O'Nan and Leonard Scott (independently) in 1979. The version I need here is little more than is in Jordan's *Traité des Substitutions* – the important extra information is all in the wreath product case.

Theorem

A finite primitive permutation group is of one of the following types: affine, wreath product, diagonal, or almost simple.

Affine groups preserve affine spaces; wreath products preserve Cartesian structures (as I discuss later); almost simple groups form a ragbag, and there is no hope for a uniform description of the structures they act on.

Our aim is to understand the geometric structure underlying diagonal groups. But, unlike in the O'Nan–Scott theorem, we do not assume that these groups are finite or primitive.

Background 1

Cheryl Praeger and Csaba Schneider started this research some time ago.

Background 1

Cheryl Praeger and Csaba Schneider started this research some time ago.

In Shenzhen in 2018, they invited Rosemary Bailey and me to join them.

Background 2

Things went on slowly, but at the six-month programme on groups at the Isaac Newton Institute in Cambridge in 2020, we hoped to bring it to a conclusion.

Background 2

Things went on slowly, but at the six-month programme on groups at the Isaac Newton Institute in Cambridge in 2020, we hoped to bring it to a conclusion.

But the coronavirus had other ideas. So we put it on hold and all went home.

An analogy

If you know any projective geometry, you will be aware of the following phenomenon:

An analogy

If you know any projective geometry, you will be aware of the following phenomenon:

- a 1-dimensional projective geometry (a projective line) has no incidence structure at all; it is just a set.

An analogy

If you know any projective geometry, you will be aware of the following phenomenon:

- a 1-dimensional projective geometry (a projective line) has no incidence structure at all; it is just a set.
- 2-dimensional projective geometries (projective planes) exist in wild profusion, so that there is no hope of classification.

An analogy

If you know any projective geometry, you will be aware of the following phenomenon:

- a 1-dimensional projective geometry (a projective line) has no incidence structure at all; it is just a set.
- 2-dimensional projective geometries (projective planes) exist in wild profusion, so that there is no hope of classification.
- For higher dimensions, a projective geometry is highly structured, and is coordinatised by an algebraic object (a division ring).

An analogy

If you know any projective geometry, you will be aware of the following phenomenon:

- a 1-dimensional projective geometry (a projective line) has no incidence structure at all; it is just a set.
- 2-dimensional projective geometries (projective planes) exist in wild profusion, so that there is no hope of classification.
- For higher dimensions, a projective geometry is highly structured, and is coordinatised by an algebraic object (a division ring).

I am going to show you that the geometries associated with diagonal groups exhibit a very similar phenomenon: "wild profusion" will mean arbitrary Latin squares, while the "algebraic object" will be a group.

An analogy

If you know any projective geometry, you will be aware of the following phenomenon:

- a 1-dimensional projective geometry (a projective line) has no incidence structure at all; it is just a set.
- 2-dimensional projective geometries (projective planes) exist in wild profusion, so that there is no hope of classification.
- For higher dimensions, a projective geometry is highly structured, and is coordinatised by an algebraic object (a division ring).

I am going to show you that the geometries associated with diagonal groups exhibit a very similar phenomenon: "wild profusion" will mean arbitrary Latin squares, while the "algebraic object" will be a group.
The analogy will be quite close: I will show you the principle which plays the role of Desargues' Theorem.

Diagonal groups

Let m be a positive integer and T a group, finite or infinite. I define the diagonal group $D(T,m)$ to be the group of permutations of $\Omega = T^m$ generated by the following transformations. (I put the elements of Ω in square brackets to distinguish them from group elements.)

Diagonal groups

Let m be a positive integer and T a group, finite or infinite. I define the diagonal group $D(T, m)$ to be the group of permutations of $\Omega = T^m$ generated by the following transformations. (I put the elements of Ω in square brackets to distinguish them from group elements.)

- The group T^m acting by right multiplication. (Let $T^m = T_1 \times \cdots \times T_m$, where T_i acts on the ith coordinate.)

Diagonal groups

Let m be a positive integer and T a group, finite or infinite. I define the diagonal group $D(T,m)$ to be the group of permutations of $\Omega = T^m$ generated by the following transformations. (I put the elements of Ω in square brackets to distinguish them from group elements.)

- The group T^m acting by right multiplication. (Let $T^m = T_1 \times \cdots \times T_m$, where T_i acts on the ith coordinate.)
- another copy T_0 of T acting by simultaneous left multiplication of all coordinates by the inverse.

Diagonal groups

Let m be a positive integer and T a group, finite or infinite. I define the diagonal group $D(T,m)$ to be the group of permutations of $\Omega = T^m$ generated by the following transformations. (I put the elements of Ω in square brackets to distinguish them from group elements.)

- The group T^m acting by right multiplication. (Let $T^m = T_1 \times \cdots \times T_m$, where T_i acts on the ith coordinate.)
- another copy T_0 of T acting by simultaneous left multiplication of all coordinates by the inverse.
- $\mathrm{Aut}(T)$ acting in the same way on all coordinates.

Diagonal groups

Let m be a positive integer and T a group, finite or infinite. I define the diagonal group $D(T, m)$ to be the group of permutations of $\Omega = T^m$ generated by the following transformations. (I put the elements of Ω in square brackets to distinguish them from group elements.)

- The group T^m acting by right multiplication. (Let $T^m = T_1 \times \cdots \times T_m$, where T_i acts on the ith coordinate.)
- another copy T_0 of T acting by simultaneous left multiplication of all coordinates by the inverse.
- $\mathrm{Aut}(T)$ acting in the same way on all coordinates.
- S_m acting by permuting the coordinates.

Diagonal groups

Let m be a positive integer and T a group, finite or infinite. I define the diagonal group $D(T,m)$ to be the group of permutations of $\Omega = T^m$ generated by the following transformations. (I put the elements of Ω in square brackets to distinguish them from group elements.)

- The group T^m acting by right multiplication. (Let $T^m = T_1 \times \cdots \times T_m$, where T_i acts on the ith coordinate.)
- another copy T_0 of T acting by simultaneous left multiplication of all coordinates by the inverse.
- $\mathrm{Aut}(T)$ acting in the same way on all coordinates.
- S_m acting by permuting the coordinates.
- An element τ:

$$[t_1, t_2, \ldots, t_m] \mapsto [t_1^{-1}, t_1^{-1}t_2, \ldots, t_1^{-1}t_m].$$

Diagonal groups

Let m be a positive integer and T a group, finite or infinite. I define the diagonal group $D(T,m)$ to be the group of permutations of $\Omega = T^m$ generated by the following transformations. (I put the elements of Ω in square brackets to distinguish them from group elements.)

- The group T^m acting by right multiplication. (Let $T^m = T_1 \times \cdots \times T_m$, where T_i acts on the ith coordinate.)
- another copy T_0 of T acting by simultaneous left multiplication of all coordinates by the inverse.
- $\mathrm{Aut}(T)$ acting in the same way on all coordinates.
- S_m acting by permuting the coordinates.
- An element τ:

$$[t_1, t_2, \ldots, t_m] \mapsto [t_1^{-1}, t_1^{-1}t_2, \ldots, t_1^{-1}t_m].$$

Don't remember the details: this is just a group built from T and m.

Partitions

Our geometry will be defined in terms of partitions. So here is a brief introduction.

Partitions

Our geometry will be defined in terms of partitions. So here is a brief introduction.

A partition of Ω can be thought of in any of three ways:

- a set of non-empty, pairwise disjoint subsets of Ω whose union is Ω;

Partitions

Our geometry will be defined in terms of partitions. So here is a brief introduction.
A partition of Ω can be thought of in any of three ways:

- a set of non-empty, pairwise disjoint subsets of Ω whose union is Ω;
- the set of equivalence classes of an equivalence relation on Ω;

Partitions

Our geometry will be defined in terms of partitions. So here is a brief introduction.
A partition of Ω can be thought of in any of three ways:

- a set of non-empty, pairwise disjoint subsets of Ω whose union is Ω;
- the set of equivalence classes of an equivalence relation on Ω;
- the kernel of a function F on Ω, that is, the set of inverse images of points in the range of F.

Partitions

Our geometry will be defined in terms of partitions. So here is a brief introduction.

A partition of Ω can be thought of in any of three ways:

- a set of non-empty, pairwise disjoint subsets of Ω whose union is Ω;
- the set of equivalence classes of an equivalence relation on Ω;
- the kernel of a function F on Ω, that is, the set of inverse images of points in the range of F.

The set $\mathbb{P}(\Omega)$ of partitions of Ω is partially ordered by refinement: $P \preccurlyeq Q$ if every part of P is contained in a part of Q.

The partition lattice

With this order, $\mathbb{P}(\Omega)$ is a lattice: any two partitions P and Q have a unique infimum or meet $P \wedge Q$, and a unique supremum or join $P \vee Q$.

The partition lattice

With this order, $\mathbb{P}(\Omega)$ is a lattice: any two partitions P and Q have a unique infimum or meet $P \wedge Q$, and a unique supremum or join $P \vee Q$.

- $P \wedge Q$ is the partition of Ω whose parts are all *non-empty* intersections of a part of P and a part of Q.

The partition lattice

With this order, $\mathbb{P}(\Omega)$ is a lattice: any two partitions P and Q have a unique infimum or meet $P \wedge Q$, and a unique supremum or join $P \vee Q$.

- $P \wedge Q$ is the partition of Ω whose parts are all *non-empty* intersections of a part of P and a part of Q.
- $P \vee Q$ is the partition into connected components of the graph in which two points are adjacent if they lie in the same part of *either* P or Q.

The partition lattice

With this order, $\mathbb{P}(\Omega)$ is a lattice: any two partitions P and Q have a unique infimum or meet $P \wedge Q$, and a unique supremum or join $P \vee Q$.

- $P \wedge Q$ is the partition of Ω whose parts are all *non-empty* intersections of a part of P and a part of Q.
- $P \vee Q$ is the partition into connected components of the graph in which two points are adjacent if they lie in the same part of *either* P or Q.

A subset of $\mathbb{P}(\Omega)$ is a sublattice if it is closed under the meet and join operations of $\mathbb{P}(\Omega)$.

The partition lattice

With this order, $\mathbb{P}(\Omega)$ is a lattice: any two partitions P and Q have a unique infimum or meet $P \wedge Q$, and a unique supremum or join $P \vee Q$.

- $P \wedge Q$ is the partition of Ω whose parts are all *non-empty* intersections of a part of P and a part of Q.
- $P \vee Q$ is the partition into connected components of the graph in which two points are adjacent if they lie in the same part of *either* P or Q.

A subset of $\mathbb{P}(\Omega)$ is a sublattice if it is closed under the meet and join operations of $\mathbb{P}(\Omega)$.
We also require the notion of a join-semilattice, closed under join but maybe not under meet.

Coset partitions

Let G be a group. For each subgroup H of G, consider the partition P_H of G into right cosets of H. We call this a coset partition.

Coset partitions

Let G be a group. For each subgroup H of G, consider the partition P_H of G into right cosets of H. We call this a coset partition.
Now, if H and K are subgroups of G, then we have

Coset partitions

Let G be a group. For each subgroup H of G, consider the partition P_H of G into right cosets of H. We call this a coset partition.
Now, if H and K are subgroups of G, then we have

- $P_H \preccurlyeq P_K$ if and only if $H \leqslant K$;

Coset partitions

Let G be a group. For each subgroup H of G, consider the partition P_H of G into right cosets of H. We call this a coset partition.

Now, if H and K are subgroups of G, then we have

- $P_H \preccurlyeq P_K$ if and only if $H \leqslant K$;
- $P_H \wedge P_K = P_{H \cap K}$;

Coset partitions

Let G be a group. For each subgroup H of G, consider the partition P_H of G into right cosets of H. We call this a coset partition.

Now, if H and K are subgroups of G, then we have

- $P_H \preccurlyeq P_K$ if and only if $H \leqslant K$;
- $P_H \wedge P_K = P_{H \cap K}$;
- $P_H \vee P_K = P_{\langle H,K \rangle}$.

Coset partitions

Let G be a group. For each subgroup H of G, consider the partition P_H of G into right cosets of H. We call this a coset partition.

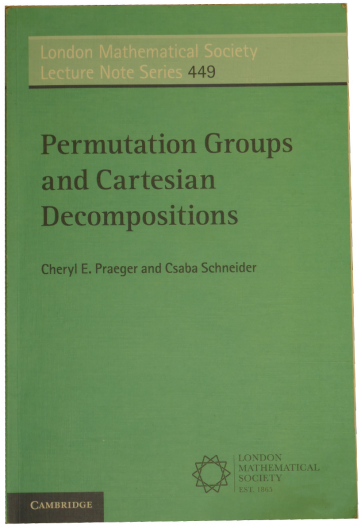
Now, if H and K are subgroups of G, then we have

- $P_H \preccurlyeq P_K$ if and only if $H \leqslant K$;
- $P_H \wedge P_K = P_{H \cap K}$;
- $P_H \vee P_K = P_{\langle H,K \rangle}$.

So the collection of all coset partitions of G forms a sublattice of $\mathbb{P}(G)$ which is isomorphic to the subgroup lattice of G, under the map $H \mapsto P_H$.

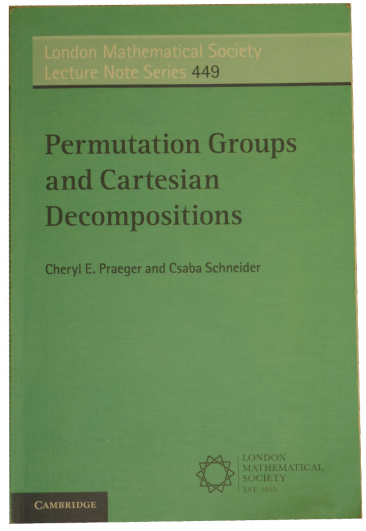
Structures for wreath products

These have many different descriptions. Praeger and Schneider, who discussed them before moving on to diagonal groups, call them Cartesian decompositions.



Structures for wreath products

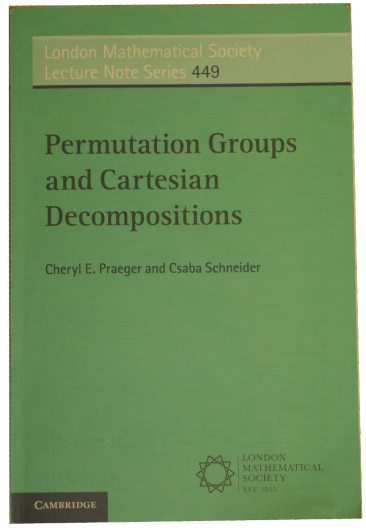
These have many different descriptions. Praeger and Schneider, who discussed them before moving on to diagonal groups, call them Cartesian decompositions.



Graph theorists call them Hamming graphs. The name hints at a connection with coding theory. Indeed, Delsarte called them Hamming schemes. This description, however, loses the order relation.

Structures for wreath products

These have many different descriptions. Praeger and Schneider, who discussed them before moving on to diagonal groups, call them Cartesian decompositions.



Graph theorists call them Hamming graphs. The name hints at a connection with coding theory. Indeed, Delsarte called them Hamming schemes. This description, however, loses the order relation.
I will use the term Cartesian lattices.

Cartesian lattices

The Boolean lattice $\mathcal{B}_n$ is the lattice of all subsets of $\{1, \ldots, n\}$.

Cartesian lattices

The Boolean lattice $\mathcal{B}_n$ is the lattice of all subsets of $\{1, \ldots, n\}$.
Let A be an alphabet, finite or infinite (with $|A| > 1$). Let
$\Omega = A^n$ be the set of all words of length n over the alphabet A.

Cartesian lattices

The Boolean lattice $\mathcal{B}_n$ is the lattice of all subsets of $\{1, \ldots, n\}$. Let A be an alphabet, finite or infinite (with $|A| > 1$). Let $\Omega = A^n$ be the set of all words of length n over the alphabet A. For $I \subseteq \{1, \ldots, n\}$, let Q_I be the partition of Ω corresponding to the equivalence relation $\equiv_I$, where

$$(a_1, \ldots, a_n) \equiv_I (b_1, \ldots, b_n) \Leftrightarrow (\forall j \notin I)(a_j = b_j).$$

Cartesian lattices

The Boolean lattice $\mathcal{B}_n$ is the lattice of all subsets of $\{1, \ldots, n\}$. Let A be an alphabet, finite or infinite (with $|A| > 1$). Let $\Omega = A^n$ be the set of all words of length n over the alphabet A. For $I \subseteq \{1, \ldots, n\}$, let Q_I be the partition of Ω corresponding to the equivalence relation $\equiv_I$, where

$$(a_1, \ldots, a_n) \equiv_I (b_1, \ldots, b_n) \Leftrightarrow (\forall j \notin I)(a_j = b_j).$$

Now the partitions Q_I for $I \subseteq \{1, \ldots, n\}$ form a sublattice of the partition lattice on Ω which is isomorphic to $\mathcal{B}_n$ by the map $I \mapsto Q_I$.

Cartesian lattices

The Boolean lattice $\mathcal{B}_n$ is the lattice of all subsets of $\{1,\ldots,n\}$.
Let A be an alphabet, finite or infinite (with $|A| > 1$). Let $\Omega = A^n$ be the set of all words of length n over the alphabet A.
For $I \subseteq \{1,\ldots,n\}$, let Q_I be the partition of Ω corresponding to the equivalence relation $\equiv_I$, where

$$(a_1,\ldots,a_n) \equiv_I (b_1,\ldots,b_n) \Leftrightarrow (\forall j \notin I)(a_j = b_j).$$

Now the partitions Q_I for $I \subseteq \{1,\ldots,n\}$ form a sublattice of the partition lattice on Ω which is isomorphic to $\mathcal{B}_n$ by the map $I \mapsto Q_I$.
I will call this a Cartesian lattice. Note that the group of permutations of Ω mapping the lattice to itself (as set of partitions) is the wreath product $\mathrm{Sym}(A)\,\mathrm{Wr}\,\mathrm{Sym}(\{1,\ldots,n\})$.

Latin squares, 1

You probably think of a Latin square as something like this: a square array of size $n \times n$ filled with letters from an alphabet of size n, so that each letter occurs once in each row and column.

Latin squares, 1

You probably think of a Latin square as something like this: a square array of size $n \times n$ filled with letters from an alphabet of size n, so that each letter occurs once in each row and column.

a	b	c
b	c	a
c	a	b

Latin squares, 1

You probably think of a Latin square as something like this: a square array of size $n \times n$ filled with letters from an alphabet of size n, so that each letter occurs once in each row and column.

a	b	c
b	c	a
c	a	b

Latin squares exist in great profusion. There are more than $\exp(m^2)$ Latin squares of order m; exact numbers are only known up to $m = 11$.

Latin squares, 1

You probably think of a Latin square as something like this: a square array of size $n \times n$ filled with letters from an alphabet of size n, so that each letter occurs once in each row and column.

a	b	c
b	c	a
c	a	b

Latin squares exist in great profusion. There are more than $\exp(m^2)$ Latin squares of order m; exact numbers are only known up to $m = 11$.
We are going to give a different definition. Let Ω consist of the n^2 cells of the array. We have three partitions of Ω: R, the rows; C, the columns; and L, the letters (the partition into sets of cells containing the same letter).

Latin squares, 2

a	b	c
b	c	a
c	a	b

1	2	3
4	5	6
7	8	9

Latin squares, 2

a	b	c
b	c	a
c	a	b

1	2	3
4	5	6
7	8	9

- $R = \{\{1,2,3\},\{4,5,6\},\{7,8,9\}\}$;
- $C = \{\{1,4,7\},\{2,5,8\},\{3,6,9\}\}$;
- $L = \{\{1,6,8\},\{2,4,9\},\{3,5,7\}\}$.

Latin squares, 2

a	b	c
b	c	a
c	a	b

1	2	3
4	5	6
7	8	9

- $R = \{\{1,2,3\},\{4,5,6\},\{7,8,9\}\}$;
- $C = \{\{1,4,7\},\{2,5,8\},\{3,6,9\}\}$;
- $L = \{\{1,6,8\},\{2,4,9\},\{3,5,7\}\}$.

Together with E (the partition into singletons) and U (the partition with a single part), these three partitions form a lattice. It has the very special property that, if one of R, C, L is omitted, the resulting four partitions form a Cartesian lattice on Ω.

Latin squares, 2

a	b	c
b	c	a
c	a	b

1	2	3
4	5	6
7	8	9

- $R = \{\{1,2,3\},\{4,5,6\},\{7,8,9\}\}$;
- $C = \{\{1,4,7\},\{2,5,8\},\{3,6,9\}\}$;
- $L = \{\{1,6,8\},\{2,4,9\},\{3,5,7\}\}$.

Together with E (the partition into singletons) and U (the partition with a single part), these three partitions form a lattice. It has the very special property that, if one of R, C, L is omitted, the resulting four partitions form a Cartesian lattice on Ω.

This property characterises Latin squares.

Latin squares, 3

With the partition definition, we could define an automorphism of a Latin square to be a permutation of Ω fixing $\{R, C, L\}$ setwise. (These mappings are usually called paratopisms in the Latin squares literature.)

Latin squares, 3

With the partition definition, we could define an automorphism of a Latin square to be a permutation of Ω fixing $\{R, C, L\}$ setwise. (These mappings are usually called paratopisms in the Latin squares literature.)
However, one case is interesting to us: the Cayley table of a group T is a Latin square, and its paratopism group is the diagonal group $D(T, 2)$ defined earlier. (This fact is maybe not as well known as it should be!)

Diagonal semilattices

Let us return to diagonal groups for a moment. Recall that $D(T, m)$ acts on T^m, where m copies $T_1, \ldots, T_m$ of T act on the corresponding coordinate of T^m by right multiplication, while the last factor T_0 acts by simultaneous left multiplication of all coordinates by the inverse.

Diagonal semilattices

Let us return to diagonal groups for a moment. Recall that $D(T, m)$ acts on T^m, where m copies $T_1, \ldots, T_m$ of T act on the corresponding coordinate of T^m by right multiplication, while the last factor T_0 acts by simultaneous left multiplication of all coordinates by the inverse.
Let $Q_0, \ldots, Q_m$ be the coset partitions of $\Omega = T^m$ corresponding to these groups. Thinking of T^m as a group, these are the coordinate partitions of the coordinate groups $T_1, \ldots, T_m$ and the diagonal subgroup of T^m (hence the name).

Diagonal semilattices

Let us return to diagonal groups for a moment. Recall that $D(T, m)$ acts on T^m, where m copies $T_1, \ldots, T_m$ of T act on the corresponding coordinate of T^m by right multiplication, while the last factor T_0 acts by simultaneous left multiplication of all coordinates by the inverse.

Let $Q_0, \ldots, Q_m$ be the coset partitions of $\Omega = T^m$ corresponding to these groups. Thinking of T^m as a group, these are the coordinate partitions of the coordinate groups $T_1, \ldots, T_m$ and the diagonal subgroup of T^m (hence the name).

The join-semilattice generated by $Q_0, \ldots, Q_m$ (it is not a lattice for $m \geqslant 3$) is an object which we will call a diagonal semilattice and denote by $\mathcal{D}(T, m)$.

Diagonal semilattices

Let us return to diagonal groups for a moment. Recall that $D(T,m)$ acts on T^m, where m copies $T_1,\dots,T_m$ of T act on the corresponding coordinate of T^m by right multiplication, while the last factor T_0 acts by simultaneous left multiplication of all coordinates by the inverse.
Let $Q_0,\dots,Q_m$ be the coset partitions of $\Omega = T^m$ corresponding to these groups. Thinking of T^m as a group, these are the coordinate partitions of the coordinate groups $T_1,\dots,T_m$ and the diagonal subgroup of T^m (hence the name).
The join-semilattice generated by $Q_0,\dots,Q_m$ (it is not a lattice for $m \geqslant 3$) is an object which we will call a diagonal semilattice and denote by $\mathcal{D}(T,m)$.

Theorem

The automorphism group of $\mathcal{D}(T,m)$ is the diagonal group $D(T,m)$.

The main theorem

Theorem

Let $m \geqslant 2$, and let $Q_0, Q_1, \ldots, Q_m$ be partitions of Ω. Suppose that any m of these partitions are the minimal non-trivial elements in an m-dimensional Cartesian lattice on Ω.

The main theorem

Theorem

Let $m \geqslant 2$, and let $Q_0, Q_1, \ldots, Q_m$ be partitions of Ω. Suppose that any m of these partitions are the minimal non-trivial elements in an m-dimensional Cartesian lattice on Ω.

- *If $m = 2$, then $\{Q_0, Q_1, Q_2\}$, together with E and U, form a Latin square, unique up to paratopism; every Latin square arises in this way.*

The main theorem

Theorem

Let $m \geqslant 2$, and let $Q_0, Q_1, \ldots, Q_m$ be partitions of Ω. Suppose that any m of these partitions are the minimal non-trivial elements in an m-dimensional Cartesian lattice on Ω.

- *If $m = 2$, then $\{Q_0, Q_1, Q_2\}$, together with E and U, form a Latin square, unique up to paratopism; every Latin square arises in this way.*
- *If $m \geqslant 3$, then there is a group T, determined up to isomorphism, such that the join-semilattice generated by $\{Q_0, \ldots, Q_m\}$ is the diagonal semilattice $\mathcal{D}(T, m)$.*

The main theorem

Theorem

Let $m \geqslant 2$, and let $Q_0, Q_1, \ldots, Q_m$ be partitions of Ω. Suppose that any m of these partitions are the minimal non-trivial elements in an m-dimensional Cartesian lattice on Ω.

- *If $m = 2$, then $\{Q_0, Q_1, Q_2\}$, together with E and U, form a Latin square, unique up to paratopism; every Latin square arises in this way.*
- *If $m \geqslant 3$, then there is a group T, determined up to isomorphism, such that the join-semilattice generated by $\{Q_0, \ldots, Q_m\}$ is the diagonal semilattice $\mathcal{D}(T, m)$.*

As promised, for $m = 2$ the situation is chaotic, but for $m \geqslant 3$ the algebraic structure coordinatising the semilattice (the group T) emerges naturally from the combinatorics.

Proof sketch

We have seen that, for $m = 2$, we get a Latin square, unique up to the natural notion of isomorphism.

Proof sketch

We have seen that, for $m = 2$, we get a Latin square, unique up to the natural notion of isomorphism.
The proof for $m \geqslant 3$ is by induction. The inductive step is not entirely trivial, requiring a little trick. But the really hard work is starting the induction at $m = 3$.

Proof sketch

We have seen that, for $m = 2$, we get a Latin square, unique up to the natural notion of isomorphism.
The proof for $m \geqslant 3$ is by induction. The inductive step is not entirely trivial, requiring a little trick. But the really hard work is starting the induction at $m = 3$.
In this case we have a special kind of Latin cube. The interval $[Q_i, U]$ in the lattice is a Latin square, and these Latin squares fit together in an intricate way. The steps are:

Proof sketch

We have seen that, for $m = 2$, we get a Latin square, unique up to the natural notion of isomorphism.
The proof for $m \geqslant 3$ is by induction. The inductive step is not entirely trivial, requiring a little trick. But the really hard work is starting the induction at $m = 3$.
In this case we have a special kind of Latin cube. The interval $[Q_i, U]$ in the lattice is a Latin square, and these Latin squares fit together in an intricate way. The steps are:

- Prove that all the Latin squares are isomorphic.

Proof sketch

We have seen that, for $m = 2$, we get a Latin square, unique up to the natural notion of isomorphism.
The proof for $m \geqslant 3$ is by induction. The inductive step is not entirely trivial, requiring a little trick. But the really hard work is starting the induction at $m = 3$.
In this case we have a special kind of Latin cube. The interval $[Q_i, U]$ in the lattice is a Latin square, and these Latin squares fit together in an intricate way. The steps are:

- Prove that all the Latin squares are isomorphic.
- Prove that one of them is a group.

Frolov and Albert

A quadrangle in a Latin square is a set of four cells lying in two rows and two columns. The square is said to satisfy the quadrangle condition if, given two quadrangles, if we can match up the cells so that three of the matched pairs are equal, then the fourth are also equal.

Frolov and Albert

A quadrangle in a Latin square is a set of four cells lying in two rows and two columns. The square is said to satisfy the quadrangle condition if, given two quadrangles, if we can match up the cells so that three of the matched pairs are equal, then the fourth are also equal.

Theorem (Frolov)

A Latin square satisfying the quadrangle condition is paratopic to the Cayley table of a group.

Frolov and Albert

A quadrangle in a Latin square is a set of four cells lying in two rows and two columns. The square is said to satisfy the quadrangle condition if, given two quadrangles, if we can match up the cells so that three of the matched pairs are equal, then the fourth are also equal.

Theorem (Frolov)

A Latin square satisfying the quadrangle condition is paratopic to the Cayley table of a group.

Theorem (Albert)

If a Latin square is paratopic to the Cayley tables of groups G_1 and G_2, then G_1 and G_2 are isomorphic.

A small mystery

Frolov proved his theorem in 1890. This was well after Dyck's axiomatisation of groups, and Cayley's construction of the Cayley table and his proof of Cayley's Theorem. But Frolov does not use the word "group", and doesn't refer to either Dyck or Cayley.

A small mystery

Frolov proved his theorem in 1890. This was well after Dyck's axiomatisation of groups, and Cayley's construction of the Cayley table and his proof of Cayley's Theorem. But Frolov does not use the word "group", and doesn't refer to either Dyck or Cayley.
He shows, in effect, that if the quadrangle condition holds then the rows of the Latin square, regarded as permutations, are closed under composition.

A small mystery

Frolov proved his theorem in 1890. This was well after Dyck's axiomatisation of groups, and Cayley's construction of the Cayley table and his proof of Cayley's Theorem. But Frolov does not use the word "group", and doesn't refer to either Dyck or Cayley.

He shows, in effect, that if the quadrangle condition holds then the rows of the Latin square, regarded as permutations, are closed under composition.

Frolov was not a professional mathematician. He was a French army officer.

A small mystery

Frolov proved his theorem in 1890. This was well after Dyck's axiomatisation of groups, and Cayley's construction of the Cayley table and his proof of Cayley's Theorem. But Frolov does not use the word "group", and doesn't refer to either Dyck or Cayley.

He shows, in effect, that if the quadrangle condition holds then the rows of the Latin square, regarded as permutations, are closed under composition.

Frolov was not a professional mathematician. He was a French army officer.

In terms of the analogy I made earlier with projective geometry, the quadrangle condition plays the role of Desargues' Theorem: most projective planes don't satisfy Desargues' theorem, but a plane embeddable in a space of higher dimension does.

The diagonal graph

There is a close connection between the Cartesian lattice and the Hamming graph. Recall that A^n is the set of words of length n over the alphabet A. The Hamming graph has vertex set A^n; two vertices are joined if as words they agree in all positions except one (that is, they have Hamming distance 1).

The diagonal graph

There is a close connection between the Cartesian lattice and the Hamming graph. Recall that A^n is the set of words of length n over the alphabet A. The Hamming graph has vertex set A^n; two vertices are joined if as words they agree in all positions except one (that is, they have Hamming distance 1).
Said otherwise, two elements of A^n are joined if they are contained in the same part of a minimal non-trivial partition of the Cartesian lattice.

The diagonal graph

There is a close connection between the Cartesian lattice and the Hamming graph. Recall that A^n is the set of words of length n over the alphabet A. The Hamming graph has vertex set A^n; two vertices are joined if as words they agree in all positions except one (that is, they have Hamming distance 1).
Said otherwise, two elements of A^n are joined if they are contained in the same part of a minimal non-trivial partition of the Cartesian lattice.
In a similar way, we can construct a graph from the diagonal semilattice: two vertices are joined if they are contained in the same part of a minimal non-trivial partition of $\mathcal{D}(T, m)$.

The diagonal graph

There is a close connection between the Cartesian lattice and the Hamming graph. Recall that A^n is the set of words of length n over the alphabet A. The Hamming graph has vertex set A^n; two vertices are joined if as words they agree in all positions except one (that is, they have Hamming distance 1).
Said otherwise, two elements of A^n are joined if they are contained in the same part of a minimal non-trivial partition of the Cartesian lattice.
In a similar way, we can construct a graph from the diagonal semilattice: two vertices are joined if they are contained in the same part of a minimal non-trivial partition of $\mathcal{D}(T, m)$.
If $m > 2$, or if $|T| > 4$, then we can reconstruct the semilattice from the graph, since the parts of the minimal partitions are cliques of size $|T|$, and conversely. It follows that the automorphism group of the diagonal graph in these cases is the same as that of the diagonal semilattice, namely the diagonal group.

We call this the diagonal graph $\Gamma_D(T, m)$. It is an interesting graph, worth further investigation. I mention a few things about it.

We call this the diagonal graph $\Gamma_D(T,m)$. It is an interesting graph, worth further investigation. I mention a few things about it.

- Except for a few very small cases, its automorphism group is the diagonal group $D(T,m)$.

We call this the diagonal graph $\Gamma_D(T, m)$. It is an interesting graph, worth further investigation. I mention a few things about it.

- Except for a few very small cases, its automorphism group is the diagonal group $D(T, m)$.
- For $m = 2$, it is a (strongly regular) Latin square graph, while for $|T| = 2$, it is a (distance-transitive) folded cube.

We call this the diagonal graph $\Gamma_D(T, m)$. It is an interesting graph, worth further investigation. I mention a few things about it.

- Except for a few very small cases, its automorphism group is the diagonal group $D(T, m)$.
- For $m = 2$, it is a (strongly regular) Latin square graph, while for $|T| = 2$, it is a (distance-transitive) folded cube.
- Except for a few very small cases, its clique number is $|T|$.

We call this the diagonal graph $\Gamma_D(T, m)$. It is an interesting graph, worth further investigation. I mention a few things about it.

- Except for a few very small cases, its automorphism group is the diagonal group $D(T, m)$.
- For $m = 2$, it is a (strongly regular) Latin square graph, while for $|T| = 2$, it is a (distance-transitive) folded cube.
- Except for a few very small cases, its clique number is $|T|$.
- If m is odd, or if $|T|$ is odd, or if the Sylow 2-subgroups of T are non-cyclic, its chromatic number is also $|T|$.

We call this the diagonal graph $\Gamma_D(T, m)$. It is an interesting graph, worth further investigation. I mention a few things about it.

- Except for a few very small cases, its automorphism group is the diagonal group $D(T, m)$.
- For $m = 2$, it is a (strongly regular) Latin square graph, while for $|T| = 2$, it is a (distance-transitive) folded cube.
- Except for a few very small cases, its clique number is $|T|$.
- If m is odd, or if $|T|$ is odd, or if the Sylow 2-subgroups of T are non-cyclic, its chromatic number is also $|T|$.

I will look briefly at the "small cases", which have $m = 2$ and $|T| \leq 4$, that is, Latin squares of order at most 4. The interesting case is order 4.

For Vijay

There are just two Latin squares of order 4, up to paratopism; these are the Cayley tables of the two groups of order 4, namely C_4 and $C_2 \times C_2$.

For Vijay

There are just two Latin squares of order 4, up to paratopism; these are the Cayley tables of the two groups of order 4, namely C_4 and $C_2 \times C_2$.

In a Latin square, there may be cliques of order 4 which are not contained in a row, column, or letter. These arise from intercalates, subsquares of order 2. I illustrate for the Cayley table of C_4.

0	**1**	2	**3**
1	2	3	0
2	**3**	0	**1**
3	0	1	2

For Vijay

There are just two Latin squares of order 4, up to paratopism; these are the Cayley tables of the two groups of order 4, namely C_4 and $C_2 \times C_2$.

In a Latin square, there may be cliques of order 4 which are not contained in a row, column, or letter. These arise from intercalates, subsquares of order 2. I illustrate for the Cayley table of C_4.

0	**1**	2	**3**
1	2	3	0
2	**3**	0	**1**
3	0	1	2

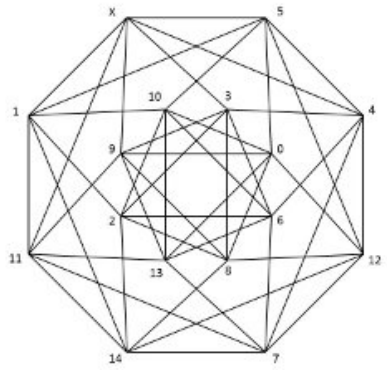
The Cayley table of C_4 contains just four intercalates. But they can be distinguished from rows, columns and letters by the fact that they intersect the other 4-cliques in zero or two vertices. So we cannot use them to reconstruct a Latin square structure.

The Shrikhande graph

Hence the automorphism group of the corresponding Latin square graph is the diagonal group $D(C_4, 2)$, with structure $(C_4 \times C_4).(\mathrm{Aut}(C_4) \times S_3)$, of order $4^2.2.6 = 192$.

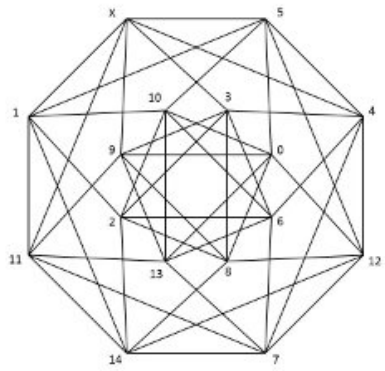
The Shrikhande graph

Hence the automorphism group of the corresponding Latin square graph is the diagonal group $D(C_4, 2)$, with structure $(C_4 \times C_4).(\mathrm{Aut}(C_4) \times S_3)$, of order $4^2.2.6 = 192$.
The complement of this Latin square graph has the same automorphism group. But this complement is the Shrikhande graph.



The Shrikhande graph

Hence the automorphism group of the corresponding Latin square graph is the diagonal group $D(C_4, 2)$, with structure $(C_4 \times C_4).(\mathrm{Aut}(C_4) \times S_3)$, of order $4^2.2.6 = 192$.
The complement of this Latin square graph has the same automorphism group. But this complement is the Shrikhande graph.



This fails for the other case $C_2 \times C_2$. This has many intercalates, and we can build a different family of cliques defining the graph. So it has twice as many automorphisms as expected (1152 instead of 576).

Chromatic number

I will say a bit more about the chromatic number of $\Gamma_D(T, m)$.

Chromatic number

I will say a bit more about the chromatic number of $\Gamma_D(T, m)$.

- There is a graph homomorphism from $\Gamma_D(T, m)$ to $\Gamma_D(T, m-2)$ (that is, a map on the vertex set taking edges to edges). Such a map cannot increase chromatic number.

Chromatic number

I will say a bit more about the chromatic number of $\Gamma_D(T, m)$.

- There is a graph homomorphism from $\Gamma_D(T, m)$ to $\Gamma_D(T, m-2)$ (that is, a map on the vertex set taking edges to edges). Such a map cannot increase chromatic number.
- $\Gamma_D(T, 1)$ is a complete graph of order $|T|$. It follows that, for odd m, the chromatic number is $|T|$.

Chromatic number

I will say a bit more about the chromatic number of $\Gamma_D(T, m)$.

- There is a graph homomorphism from $\Gamma_D(T, m)$ to $\Gamma_D(T, m-2)$ (that is, a map on the vertex set taking edges to edges). Such a map cannot increase chromatic number.
- $\Gamma_D(T, 1)$ is a complete graph of order $|T|$. It follows that, for odd m, the chromatic number is $|T|$.
- For m even, we have $\chi(\Gamma_D(T, m)) \leq \chi(\Gamma_D(m, 2))$, where $\Gamma_D(m, 2)$ is the Latin square graph of the Cayley table of T.

Chromatic number

I will say a bit more about the chromatic number of $\Gamma_D(T, m)$.

- There is a graph homomorphism from $\Gamma_D(T, m)$ to $\Gamma_D(T, m-2)$ (that is, a map on the vertex set taking edges to edges). Such a map cannot increase chromatic number.
- $\Gamma_D(T, 1)$ is a complete graph of order $|T|$. It follows that, for odd m, the chromatic number is $|T|$.
- For m even, we have $\chi(\Gamma_D(T, m)) \leq \chi(\Gamma_D(m, 2))$, where $\Gamma_D(m, 2)$ is the Latin square graph of the Cayley table of T.
- If the Cayley table has an orthogonal mate, this is a colouring of the graph with $|T|$ colours.

Chromatic number

I will say a bit more about the chromatic number of $\Gamma_D(T, m)$.

- There is a graph homomorphism from $\Gamma_D(T, m)$ to $\Gamma_D(T, m-2)$ (that is, a map on the vertex set taking edges to edges). Such a map cannot increase chromatic number.
- $\Gamma_D(T, 1)$ is a complete graph of order $|T|$. It follows that, for odd m, the chromatic number is $|T|$.
- For m even, we have $\chi(\Gamma_D(T, m)) \leq \chi(\Gamma_D(m, 2))$, where $\Gamma_D(m, 2)$ is the Latin square graph of the Cayley table of T.
- If the Cayley table has an orthogonal mate, this is a colouring of the graph with $|T|$ colours.
- By the Hall–Paige conjecture, whose proof depends on the classification of finite simple groups, the Cayley table of T has an orthogonal mate if and only if either $|T|$ is odd or T has non-cyclic Sylow 2-subgroups.

Chromatic number

I will say a bit more about the chromatic number of $\Gamma_D(T, m)$.

- There is a graph homomorphism from $\Gamma_D(T, m)$ to $\Gamma_D(T, m-2)$ (that is, a map on the vertex set taking edges to edges). Such a map cannot increase chromatic number.
- $\Gamma_D(T, 1)$ is a complete graph of order $|T|$. It follows that, for odd m, the chromatic number is $|T|$.
- For m even, we have $\chi(\Gamma_D(T, m)) \leq \chi(\Gamma_D(m, 2))$, where $\Gamma_D(m, 2)$ is the Latin square graph of the Cayley table of T.
- If the Cayley table has an orthogonal mate, this is a colouring of the graph with $|T|$ colours.
- By the Hall–Paige conjecture, whose proof depends on the classification of finite simple groups, the Cayley table of T has an orthogonal mate if and only if either $|T|$ is odd or T has non-cyclic Sylow 2-subgroups.
- If this is not the case, then it is conjectured that the chromatic number of $\Gamma_D(T, 2)$ is $|T| + 2$, and we conjecture that the same holds for $\Gamma_D(m, 2)$ for all even m.

The 1-dimensional case

I mentioned that the method we have used to define geometry for a diagonal group fails when $m = 1$. The diagonal group $D(T, 1)$ is not without interest. It is a group acting on T; the two factors T act, one by right and one by left multiplication; we also have automorphisms of T and the inverse map.

The 1-dimensional case

I mentioned that the method we have used to define geometry for a diagonal group fails when $m = 1$. The diagonal group $D(T, 1)$ is not without interest. It is a group acting on T; the two factors T act, one by right and one by left multiplication; we also have automorphisms of T and the inverse map.
In 1968, Peter Neumann, Charles Sims and James Wiegold published a paper with the wonderful title "Counterexamples to a theorem of Cauchy".

The 1-dimensional case

I mentioned that the method we have used to define geometry for a diagonal group fails when $m = 1$. The diagonal group $D(T, 1)$ is not without interest. It is a group acting on T; the two factors T act, one by right and one by left multiplication; we also have automorphisms of T and the inverse map.

In 1968, Peter Neumann, Charles Sims and James Wiegold published a paper with the wonderful title "Counterexamples to a theorem of Cauchy".

Their counterexamples were diagonal groups $D(T, 1)$, where T is simple.

Cauchy had "proved" that, if a primitive group has degree a prime number plus one, then the group must be doubly transitive. Neumann, Sims and Wiegold pointed out that, if T is a finite simple group, then $D(T, 1)$ is primitive but not doubly transitive.

Cauchy had "proved" that, if a primitive group has degree a prime number plus one, then the group must be doubly transitive. Neumann, Sims and Wiegold pointed out that, if T is a finite simple group, then $D(T, 1)$ is primitive but not doubly transitive.

There are many simple groups whose order is one more than a prime:

Cauchy had "proved" that, if a primitive group has degree a prime number plus one, then the group must be doubly transitive. Neumann, Sims and Wiegold pointed out that, if T is a finite simple group, then $D(T, 1)$ is primitive but not doubly transitive.

There are many simple groups whose order is one more than a prime:

- $|A_5| = 59 + 1$;

Cauchy had "proved" that, if a primitive group has degree a prime number plus one, then the group must be doubly transitive. Neumann, Sims and Wiegold pointed out that, if T is a finite simple group, then $D(T, 1)$ is primitive but not doubly transitive.

There are many simple groups whose order is one more than a prime:

- $|A_5| = 59 + 1$;
- $|\mathrm{PSL}(2, 7)| = 167 + 1$;

Cauchy had "proved" that, if a primitive group has degree a prime number plus one, then the group must be doubly transitive. Neumann, Sims and Wiegold pointed out that, if T is a finite simple group, then $D(T, 1)$ is primitive but not doubly transitive.

There are many simple groups whose order is one more than a prime:

- $|A_5| = 59 + 1$;
- $|\mathrm{PSL}(2, 7)| = 167 + 1$;
- $|A_6| = 359 + 1$;

Cauchy had "proved" that, if a primitive group has degree a prime number plus one, then the group must be doubly transitive. Neumann, Sims and Wiegold pointed out that, if T is a finite simple group, then $D(T, 1)$ is primitive but not doubly transitive.

There are many simple groups whose order is one more than a prime:

- $|A_5| = 59 + 1$;
- $|\mathrm{PSL}(2, 7)| = 167 + 1$;
- $|A_6| = 359 + 1$;
- $|\mathrm{PSL}(2, 8)| = 503 + 1$;

Cauchy had "proved" that, if a primitive group has degree a prime number plus one, then the group must be doubly transitive. Neumann, Sims and Wiegold pointed out that, if T is a finite simple group, then $D(T, 1)$ is primitive but not doubly transitive.

There are many simple groups whose order is one more than a prime:

- $|A_5| = 59 + 1$;
- $|\mathrm{PSL}(2, 7)| = 167 + 1$;
- $|A_6| = 359 + 1$;
- $|\mathrm{PSL}(2, 8)| = 503 + 1$;

and so on.

Cauchy had "proved" that, if a primitive group has degree a prime number plus one, then the group must be doubly transitive. Neumann, Sims and Wiegold pointed out that, if T is a finite simple group, then $D(T,1)$ is primitive but not doubly transitive.

There are many simple groups whose order is one more than a prime:

- $|A_5| = 59 + 1$;
- $|\mathrm{PSL}(2,7)| = 167 + 1$;
- $|A_6| = 359 + 1$;
- $|\mathrm{PSL}(2,8)| = 503 + 1$;

and so on.

A challenge to number theorists: Are there infinitely many finite simple groups which give counterexamples to Cauchy's theorem in this way?

More partitions

A set of $r+2$ partitions, any two of which are the minimal elements in a 2-dimensional Cartesian lattice, is nothing but a set of r mutually orthogonal Latin squares. These are classical objects going back to Euler, if not earlier.

More partitions

A set of $r+2$ partitions, any two of which are the minimal elements in a 2-dimensional Cartesian lattice, is nothing but a set of r mutually orthogonal Latin squares. These are classical objects going back to Euler, if not earlier.
We have begun investigating sets of $m+r$ partitions, any m of which are the minimal elements in an m-dimensional Cartesian lattice, for $r \geq 2$. Then by our main theorem, any $m+1$ of the partitions are the minimal elements in a diagonal semilattice $\mathcal{D}(T,m)$ for some group T. One rather basic question which we can't answer is:

Problem

If $r > 1$, are all the groups T arising from sets of $m+1$ partitions isomorphic?

More partitions

A set of $r+2$ partitions, any two of which are the minimal elements in a 2-dimensional Cartesian lattice, is nothing but a set of r mutually orthogonal Latin squares. These are classical objects going back to Euler, if not earlier.
We have begun investigating sets of $m+r$ partitions, any m of which are the minimal elements in an m-dimensional Cartesian lattice, for $r \geq 2$. Then by our main theorem, any $m+1$ of the partitions are the minimal elements in a diagonal semilattice $\mathcal{D}(T,m)$ for some group T. One rather basic question which we can't answer is:

Problem

If $r > 1$, are all the groups T arising from sets of $m+1$ partitions isomorphic?

This is false in the case $m = 2$, even if all the Latin squares are Cayley tables of groups.

The paper containing the main theorem is:

- R. A. Bailey, Peter J. Cameron, Cheryl E. Praeger, Csaba Schneider, The geometry of diagonal groups, *Trans. Amer. Math. Soc.*, in press; arXiv 2007.10726

Related papers:

- R. A. Bailey, Peter J. Cameron, Michael Kinyon and Cheryl E. Praeger, Diagonal groups and arcs over groups, *Designs, Codes, Cryptography*, in press; arXiv 2010.16338.
- R. A. Bailey and Peter J. Cameron, The diagonal graph, *J. Ramanujan Math. Soc.*, in press; arXiv 2101.02451
- J. N. Bray, P. J. Cameron, Q. Cai, P. Spiga and H. Zhang, The Hall–Paige conjecture, and synchronization for affine and diagonal groups, *J. Algebra* **545** (2020), 27-42; arXiv 1811.12671

The paper containing the main theorem is:

- R. A. Bailey, Peter J. Cameron, Cheryl E. Praeger, Csaba Schneider, The geometry of diagonal groups, *Trans. Amer. Math. Soc.*, in press; arXiv 2007.10726

Related papers:

- R. A. Bailey, Peter J. Cameron, Michael Kinyon and Cheryl E. Praeger, Diagonal groups and arcs over groups, *Designs, Codes, Cryptography*, in press; arXiv 2010.16338.
- R. A. Bailey and Peter J. Cameron, The diagonal graph, *J. Ramanujan Math. Soc.*, in press; arXiv 2101.02451
- J. N. Bray, P. J. Cameron, Q. Cai, P. Spiga and H. Zhang, The Hall–Paige conjecture, and synchronization for affine and diagonal groups, *J. Algebra* **545** (2020), 27-42; arXiv 1811.12671